Notice of Allowability	Application No.	Applicant(s)	
	10/615,278	DEAVER ET AL.	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *17 July 2007*.

2. ☒ The allowed claim(s) is/are *1-4,6,8-14,16,18-24,26 and 28-30*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 17 July 2007
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. A Request for Continued Examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 17 July 2007 has been entered and respectfully and carefully considered.

2. As a result of the amendment, claims 1, 11 and 21have been amended. Therefore, claims 1-4, 6-14, 16-24 and 26-30 are currently pending in the present application.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Paul Kudirka on 29 August 2007.

- Please cancel **claims 7, 17 and 27**
- Please replace the claims as follows:

1. (Currently Amended) A method for secure key delivery for decrypting a distribution archive file containing a plurality of digital content documents

at an unsecured site that receives a stream of distribution archive files from a publishing site, the method comprising:

(a) at the publishing site, encrypting each digital content document with a key to generate encrypted document content;

(b) at the publishing site, computing for each document a document identifier that is computed from, but cannot be derived solely from, the encrypted content of that document, wherein the document identifier is computed using a text string embedded in program code in the publishing site;

(c) at the publishing site, creating a list of document identifier and decryption key pairs;

(d) at the publishing site, assembling the encrypted document content for each content document and the key pair list into a distribution archive file;

(e) at the publishing site, encrypting the distribution archive file with a scheduled key unique to that distribution archive file and placing the encrypted distribution file on the stream;

(f) at the unsecured site, selecting a distribution archive file from the stream;

(g) at the unsecured site, extracting a scheduled key from the selected distribution archive file in the stream;

(h) at the unsecured site, using the extracted scheduled key to decrypt the next subsequent distribution archive file in the stream following the selected distribution archive file;

(i) removing the encrypted document content and the key pair list from the decrypted distribution archive file and storing them at the unsecured site;

(j) selecting the distribution archive file decrypted in step (h); and

(k) repeating steps (g), (h), (i) and (j) for each distribution archive file in the stream.

2. (Currently Amended) The method of claim 1 further comprising:

(l) receiving a scheduled key at the unsecured site to decrypt the first distribution archive file in the stream from the publishing site.

8. (Currently Amended) The method of claim 1 wherein step (g) comprises temporarily storing an extracted scheduled key in encrypted form.

9. (Currently Amended) The method of claim ~~7~~ 1 further comprising recomputing a document identifier at the unsecured site with a text string embedded in program code located at the unsecured site.

11. (Currently Amended) An apparatus for secure key delivery for decrypting a distribution archive file containing a plurality of digital content documents

at an unsecured site that receives a stream of distribution archive files from a publishing site, the apparatus comprising:

at the publishing site, an encryption engine that encrypts each digital content document with a key to generate encrypted document content;

at the publishing site, an OID calculator that computes for each document a document identifier that is computed from, but cannot be derived solely from, the encrypted content of that document, wherein the document identifier is computed using a text string embedded in program code in the publishing site;

at the publishing site, means for creating a list of document identifier and decryption key pairs;

at the publishing site, means for assembling the encrypted document content for each content document and the key pair list into a distribution archive;

at the publishing site, means for encrypting the distribution archive file with a scheduled key unique to that distribution archive file;

at the unsecured site, a key decryptor that extracts a scheduled key from each distribution archive file in the stream;

means for temporarily storing the extracted scheduled key at the unsecured site;

at the unsecured site, a decryption engine that uses the stored scheduled key to decrypt the next distribution archive file in the stream

following the distribution archive file from which the scheduled key was extracted; and

a file system that removes the encrypted document content and the key pair list from the decrypted archive file and stores them at the unsecured site.

19. (Currently Amended) The apparatus of claim ~~17~~ 11 further comprising means for recomputing a document identifier with a text string embedded in program code located at the unsecured site.

21. (Currently Amended) A computer program product for secure key delivery for decrypting a distribution archive file containing a plurality of digital content files at an unsecured site that receives a stream of distribution archive files from a publishing site, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code at the publishing site, for encrypting each digital content document with a key to generate encrypted document content;

program code at the publishing site, for computing for each document a document identifier that is computed from, but cannot be derived solely from, the encrypted content of that document, wherein the

document identifier is computed using a text string embedded in program code in the publishing site;

program code at the publishing site, for creating a list of document identifier and decryption key pairs;

program code at the publishing site, for assembling the encrypted document content for each content document and the key pair list into a distribution archive file; and

program code at the publishing site, for encrypting the distribution archive file with a scheduled key unique to that distribution archive file and for placing the encrypted distribution file on the stream;

program code at the unsecured site for extracting a scheduled key from each distribution archive file in the stream;

program code at the unsecured site for temporarily storing the extracted scheduled key;

program code at the unsecured site for using the stored scheduled key to decrypt the next distribution archive file in the stream following the distribution archive file from which the scheduled key was extracted; and

program code for removing the encrypted document content and the key pair list from the decrypted archive file and for storing them at the unsecured site.

29. (Currently Amended) The computer program product of claim ~~28~~ 21 further comprising program code for recomputing a document identifier with a text string embedded in program code located at the unsecured site.

Allowable Subject Matter

4. Claims 1-4, 6, 8-14, 16, 18-24, 26 and 28-30 are allowed.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

30 August 2007
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100